

ORIGINAL

DEFINITY

National DEFINITY® Users Group, Inc. P.O. Box 2167 • Indianapolis, Indiana 46206-2167

President

Keith Frank

The University of Oklahoma
College of Medicine
2808 S. Sheridan Road
Tulsa OK 74129
918-838-4709

RECEIVED

JAN 14 1994

January 13, 1994

FCC MAIL ROOM

Mr. William F. Caton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Caton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As President of the National DEFINITY Users Group, I am encouraged by the proposed rulemaking because even though I and the 1,500 members of my organization have taken each and every protective step recommended by the IXC's and CPE vendors to secure our systems, we can still experience toll fraud. It is impossible to secure our systems 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car, not as an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is

No. of Copies rec'd 054
List A B C D E

superficial. Monitoring by the IXC's should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXC's were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LEC's should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe that hackers only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

A handwritten signature in black ink, appearing to read "Keith Frank", with a long, sweeping horizontal line extending to the right.

Keith Frank, President

Hewlett-Packard Company
20 New England Avenue
Piscataway, New Jersey 08854



January 13, 1994

Office of the Secretary
Federal Communications Commission
Washington, D.C. 20554

RECEIVED

JAN 14 1994

FCC MAIL ROOM

To Whom It May Concern:

Enclosed please find comments relating to Docket Number 93-292 dealing with network fraud. Hewlett-Packard Company would like to request exparte communications with a committee associated with this issue. Following a conversation last week, I have sent a copy of this package to Ms. Linda Dubroof asking her to contact me regarding the necessary steps for setting up such a meeting.

Sincerely,

Hewlett-Packard Company

A handwritten signature in cursive script, appearing to read "Peter R. Rogina".

Peter R. Rogina
Communications Systems Business Manager

No. of Copies rec'd
List A B C D E

008

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the matter of
Policies and Rules
concerning Toll Fraud

)
) CC Docket No. 93-292
)

RECEIVED
JAN 14 1994
FCC MAIL ROOM

NOTICE OF PROPOSED RULEMAKING

The following are the comments of Hewlett-Packard Company in response to the Federal Communications Commission request regarding the availability of technologies capable of providing early detection and warning of the occurrence of fraud activities within the telecommunications network.

It is not our intent to become involved in the discussion as to how losses should be distributed, nor to become involved in the specific wording to be used to warn customers of the potential of fraud. These issues are being addressed by the proper groups.

It is the intent of Hewlett-Packard to share information relative to new technology which will allow network operators to recognize fraudulent calling patterns in near real-time, thus allowing them to identify and quickly address many different types of fraud. After a full understanding of the way that the current technology and architecture can address the problem of fraud in the telecommunications industry, it is our hope that aggressive measures be considered by the FCC to hold network operators liable for certain types of fraud plaguing customers in the United States. Further, we request the opportunity to have formal exparte communications with a committee associated with this issue so as to further describe the method becoming available to combat fraud in the network.

Until recently, the capability of a telecommunications service provider to detect the occurrence of fraud has been limited. In those cases where a telecommunications provider has control of key portions of the network, such as Line Information Data Base (LIDB) information, steps have been taken to minimize the occurrence of fraud. All LIDB operators have implemented software capable of providing reasonable fraud detection capabilities. The nature of the fraudster is such that as they become aware of the ability to detect their presence, they simply devise a new method of attack or refocus their energies elsewhere.

Historically, the primary tool used by telecommunications providers to detect fraud activities has been based upon the review of billing records. The disadvantage of this approach is that the records are not presented in real time. Often the captured data would be weeks old prior to processing. Under very specific circumstances the data can be processed in near real time, however, the capability to perform this level of processing on a large scale is limited.

Customer Premise Equipment (CPE) systems have emerged, intended to be installed at the customer location. These systems are sized to accommodate the small number of trunks which typically support a PBX customers needs. Not all customer premises equipment users have installed the available systems, nor have potential solutions, such as limiting system access and egress or requesting of denial of international calls, been implemented by all of the end users (i.e. 89% of PBX users do not normally place international calls, however, fraudulent international calling from compromised PBX's is a very expensive problem).

Systems which reside within the Service Providers networks gather information primarily (if not completely) from the switches or other network elements (NE's). This is the same way that the information used to generate bills is captured. In the case of billing, the information is passed to a processor which aggregates and generates the bills. Similarly, Network Monitoring systems rely on these same network elements to pass on the vital network data, albeit in a more real-time manner (hopefully). In reality, if a network element begins to become congested due to a high call throughput rate, one of the first things to be compromised is the passing of data out of the element. The priority is for the switch to process the calls. One key issue facing NE manufacturers is trying to design their equipment to process the amount of information that they are being asked to report on. This must occur while simultaneously handling the more complex capabilities required at the much higher speeds appearing in the network. Another difficulty arises if a latent bug in a version of software that resides on the switch affects the data leaving that switch.

A system used to detect fraud which gathers its information directly from the NE's is subject to the same potential limitations as those described above. This has the effect of potentially making the system less reliable and less easy to modify and/or update. New versions of software are only put onto switches a few times a year at best and only after diligent testing, therefore the ability to quickly adjust to new types of fraud would be limited

In response to the request for technologies capable of providing early detection and warning of the occurrence of fraud, we wish to respond indicating that we have recognized the need for an advanced method for fraud detection and are involved in the development the such a system. The approach which we are taking is based upon use of the protocol implemented within the SS7 network(s).

Today SS7 network(s) are used universally to establish the communications channels. Virtually all toll calls in the US transverse the various SS7 networks developed by the telecommunications service providers. SS7 is defined in internationally recognized standards, and permits network interworking independent of switch vendor.

The HP system operation is protocol based, deriving the required information from the actual SS7 messages used to establish and control the required communications channel. Included within the various messages which are a part of the SS7 protocol is data which can be used to provide detection of calling patterns.

SS7 based fraud detection systems offer the following benefits. Firstly, they are capable of being readily modified to detect new forms of fraudulent behavior and fraud in new services. For example, cellular phone calls set up by the CTIA IS.41 call control infrastructure which is SS7 based and future Advanced Intelligent Network (AIN) services. Secondly, this approach supports true near real-time fraud detection capabilities across an entire network.

Through HP's involvement in various industry fraud conferences, we have learned many of the methods used to defraud network operators and have evaluated many of those methods relative to the SS7 approach to fraud detection. The results are very encouraging and we would welcome the opportunity to further discuss the potential advantages of this type of detection scheme with the committee at a future date. There are currently plans to present papers on this subject at upcoming industry forums.

Information collected from the SS7 signaling links could be "re-formatted" so as to look like information coming from a specific NE. This would allow the use of existing fraud software, thereby protecting a large portion of the investment many companies may have made in software algorithms. New algorithms will surely evolve and be designed as to work efficiently in the described architecture.

Given the potential capabilities of SS7-based fraud detection systems, Hewlett-Packard strongly encourages the FCC to be aggressive in formulating the policies which hold the network operators responsible for losses incurred due to fraud.

Definition of acronyms:

CTIA - Cellular Technology Industry Association

IS.41 - CTIA specification for a Cellular Radio Telecommunications Intersystems Operations Protocol



Metropolitan Transportation Authority

347 Madison Avenue
New York, NY 10017
Telephone: 212 340-3000

JAN 14 1994

January 13, 1994 FCC MAIL ROOM

Office of the Secretary
Federal Communications Commission
Washington, DC 20554

Re: CC Docket 93-292 Comments on Polices and Rules
Concerning Toll Fraud

Dear Mr. Secretary:

I am writing on behalf of Metro-North Commuter Railroad ("Metro-North") to offer comments in response to the December 2, 1993 Notice of Proposed Rulemaking issued by the Federal Communications Commission on the subject of telephone toll fraud. Metro-North is a taxpayer-subsidized public benefit corporation of the State of New York, and a subsidiary of the Metropolitan Transportation Authority. We are the nation's second largest commuter railroad and the backbone of public transportation for the northern portion of the New York metropolitan area. Our 338-mile system extends into New York City and Westchester, Putnam, Dutchess, Orange and Rockland counties in New York State, and Fairfield and New Haven counties in Connecticut.

Warnings Should be Required

Like a growing number of businesses, Metro-North has been a victim of high volume toll fraud by unauthorized callers from off-premises locations who gained access to our PBX system via an AT&T 800 number intended for use by employees only. At present, Metro-North is defending a federal court action brought by AT&T to recover \$213,639.12 in charges for such unauthorized calls. Metro-North was unaware that unauthorized callers from remote locations could gain access to our outward dialing trunks via AT&T's 800 number and the PBX system. And, we believe that the fraud against Metro-North could have been avoided, or at least drastically reduced, had we been properly informed of standard precautionary measures needed to secure our telephone system. Accordingly, Metro-North strongly urges the FCC to affirmatively conclude that

Members of the Board

Peter E. Stangl
Chairman and
Chief Executive Officer
Daniel T. Scannell
First Vice Chairman

Lilyan H. Affinito
Bernard B. Beal
E. Virgil Conway
Warren S. Dolny
Barry L. Feinstein

Barbara J. Fife
Sally Hernandez-Pinero
Herbert J. Libert
Prem Mathai-Davis
Neil Novesky

Lucius J. Riccio
Joan Spence
Edward A. Vrooman

Donald N. Nelson
President

No. of Copies rec'd
List A B C D E

Donald N. Nelson
resident

tariff liability provisions that fail to recognize an obligation by the carrier to warn customers of risks is unreasonable. As a public benefit corporation receiving funds from the State of New York and the federal government, it is particularly important that we, and similar public entities, be fully informed to ensure that we can protect against losses.

Specific Nature of Warnings

Metro-North proposes that all applicable contract documents, written training materials, and service sessions contain specific language describing the potential use of 800 numbers by unauthorized users to gain access to an internal PBX system. In addition, a specific document created expressly for the purpose of providing this information should be given to all new subscribers. The same documents and training sessions should also provide specific information on fraud prevention techniques, and/or where to obtain such information. The fraud prevention information should specify the minimum actions necessary to avoid liability for unauthorized charges.

Other Prevention Techniques

Metro-North also proposes that carriers, at no cost to the customer, be required to monitor inbound and outbound calls, and to report unusual calling patterns to the customer within 24 hours of determining that such a pattern exists. Carriers should also be required to offer users the option to block incoming and/or outgoing calls, per a customer's request, and be required to offer special educational services, at an additional cost to the customer.

Dispute Resolution

With the above-described safeguards in place, there is a parallel obligation on the customer to implement the minimum recommended fraud prevention techniques. Where fraud occurs, liability should be apportioned based on comparative fault in complying with respective obligations. Metro-North strongly supports the use of alternative dispute resolution procedures in the event of unauthorized use charges. We recommend that the FCC require, at a minimum, exhaustion of FCC administrative procedures prior to initiating an action in court to recover charges for unauthorized calls. Ideally, the administrative procedure would at least encourage the parties to seek mediation or arbitration of the dispute, with the parties to share the costs of the process chosen.

Office of the Secretary
January 13, 1994
Page Three

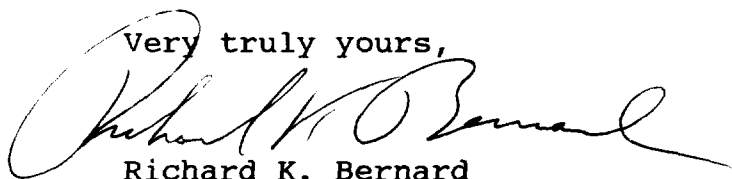
Guidelines for Settlement of Pending Litigation

One final issue which needs attention is the resolution of litigation now pending throughout the country on PBX fraud. While some district courts, relying on the Chartways decision, have issued rulings placing full liability with the customer, the present rulemaking process casts doubt on the continued validity of these district court decisions. While the FCC may not have the authority to order that all pending actions by carriers for PBX toll fraud charges be settled by the carriers according to a particular formula, Metro-North urges that the FCC issue guidelines for suggested settlements. Specifically, where no warnings were given to the customer, Metro-North requests the FCC to recommend that the carrier absorb the full amount of the unauthorized charges.

Metro-North supports the FCC's commitment to controlling telephone toll fraud by clearly defining carrier and customer obligations, as well as by making certain customers are apprised of the means available to secure telephone systems. It is only through taking these steps that the interests of the public will be protected, and costly litigation avoided.

Thank you for your attention.

Very truly yours,

A handwritten signature in black ink, appearing to read "Richard K. Bernard", written over the typed name.

Richard K. Bernard
General Counsel

cc: U. S. Representative Edward J. Markey
U. S. Representative James . Scheuer
U. S. Representative Thomas J. Manton